DAHLGREN DIVISION
NAVAL SURFACE WARFARE CENTER
Dahlgren, Virginia 22448-5100

NSWCDD/TR-96/217

WEAPON SYSTEM SAFETY: BRIDGING THE GAP BETWEEN HARDWARE AND SOFTWARE

BY MICHAEL ZEMORE

WEAPONS SYSTEMS DEPARTMENT

JANUARY 1997

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE
January 1997

3. REPORT TYPE AND DATES COVERED
Final

4. TITLE AND SUBTITLE
Weapon System Safety: Bridging the Gap Between Hardware and Software

5. FUNDING NUMBERS

6. AUTHOR(s)
Michael Zemore

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Commander
Naval Surface Warfare Center
Dahlgren Division (Code G71)
17320 Dahlgren Road
Dahlgren, VA 22448-5100

8. PERFORMING ORGANIZATION REPORT NUMBER
NSWCDD/TR-96/217

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)
System safety efforts for major weapon systems often provide for the early identification of hazards and the elimination or control of those hazards through system design. Although this process has been proven effective in providing safe and effective weapon systems, significant deficiencies exist when computer programs utilized within the system are not adequately addressed. With the influx of computer programs in today's weapon system designs, it is critical to ensure computer program safety analysis is integrated into the system safety analysis process. With the proper analysis effort for all aspects of the system, and the proper integration of those efforts, a thorough identification and resolution of hazards will occur whether those hazards are induced by a failure mode, adverse environment, or computer program condition.

This report addresses a system safety methodology and flow of safety-related information from system-related analyses to computer-program-related analyses. Specifically, the identification of safety-critical functions, analysis techniques, and the identification of potential hazards in computer programs are discussed. In addition, a method for accurately assessing risk associated with computer program hazards and documenting their relationship to system-level events is defined.

14. SUBJECT TERMS
Safety Analysis Process, Computer Program Safety Analysis, Subsystem Hazard Analysis, Event Criticality List, Preliminary Hazards List, Preliminary Hazard Analysis

15. NUMBER OF PAGES
25

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORTS	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev 2-89)
Prescribed by ANSI std. Z39-18

FOREWORD

The information and methodology provided in this report were developed under the guidance of Senior Systems Safety Engineers of the Naval Surface Warfare Center, Dahlgren Division (NSWCDD). Specifically, Johnson B. Gessler, Combat Systems Safety and Engineering Division (G705), Harley P. Dixon, Systems Safety Engineering Branch (G71), and Robert K. Baeder, Systems Safety Engineering Branch (G71), contributed significantly toward the development of these processes and the documentation thereof.

This document has been reviewed by Michael S. Ramsburg, Head, Systems Safety Engineering Branch, and Gary C. Blount, Head, Combat Systems Safety and Engineering Division.

Approved by:

David S. Malyevac

DAVID S. MALYEVAC, Deputy Head
Weapons Systems Department

CONTENTS

ILLUSTRATIONS

TABLES

NOMENCLATURE

CFL	Critical Functions List
CPSA	Computer Program Safety Analysis
ECL	Event Criticality List
FMHEA	Failure Modes And Hazardous Effects Analysis
FTA	Fault Tree Analysis
O&SHA	Operating And Support Hazard Analysis
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazards List
RA	Risk Assessment
SAP	Safety Analysis Process
SSHA	Subsystem Hazard Analysis
SR	Safety Requirement

1.0 INTRODUCTION

System safety is the process of identifying hazards and mitigating risks related to those hazards. The safety effort begins at the earliest phases of a weapon system's life and continues throughout its entire life-cycle. The process involves all aspects of the weapon system, including computer programs. For the purposes of this report, a Safety Analysis Process (SAP) is defined which demonstrates the integral aspects of performing system safety analyses and detailed Computer Program Safety Analyses (CPSAs). The SAP is especially effective when various agencies are tasked with subsystem safety responsibilities, or the life of a weapon system spans several years.

2.0 SAFETY ANALYSIS PROCESS

The SAP, as shown in Figure 1, provides a unified approach to system safety while establishing a mechanism for assessing risk associated with computer program deficiencies. Although computer programs are often addressed as "components" within system or subsystem hazard analyses, the analyses often fail to address the specifics of the computer programs themselves. Likewise, computer program hazard analyses are often conducted without system knowledge or an understanding of known hazardous states. The SAP overcomes these known safety analysis deficiencies.

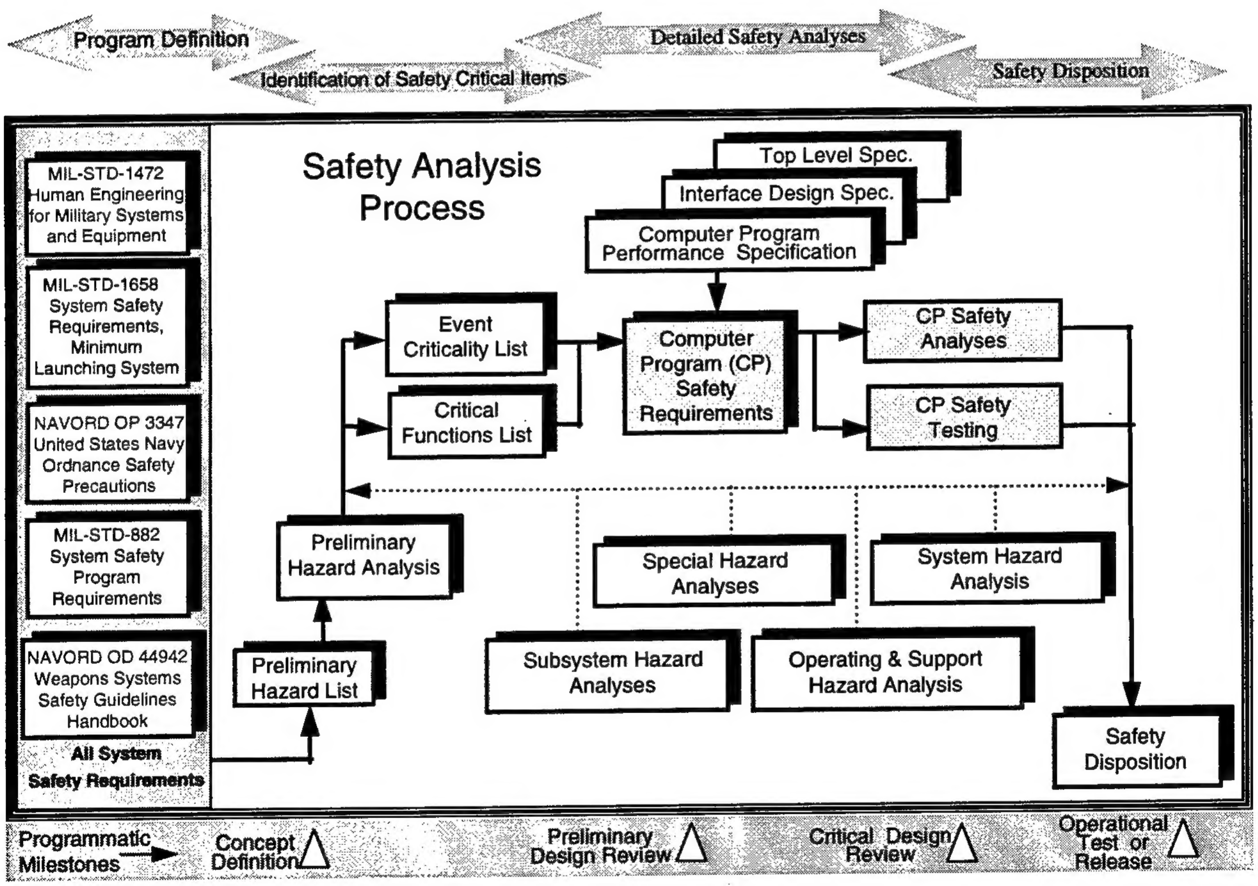

Figure 1. Safety Analysis Process

The SAP illustrates the relationships between the system related hazard analyses and the detailed CPSA efforts. It also defines safety data items necessary for the unification of system safety efforts. The programmatic milestones are identified only as a guideline for establishing timeframes for safety related analysis efforts. The SAP is broken into four basic phases. The first phase establishes the safety program and identifies the guidelines to be used for the safety program. The second phase initiates system level hazard analyses for the weapon system under development. Specific safety data items are documented during this time as a result of hazard analysis efforts. These items are the Event Criticality List (ECL) and the safety Critical Functions List (CFL). The ECL documents the adverse weapon system safety events with their determined severities and the CFL documents all weapon system safety critical functions. This phase is critical to the CPSA efforts since these safety data items provide the main focus and sensitivity for CPSA efforts. The data items also provide the basis for assessing hazards and determining risk associated with computer program coding deficiencies. Phase three provides for detailed safety analyses of preliminary and formal designs. This phase is where specific hazards associated with proposed designs are identified and resolved through safety engineering recommendations and design changes. The final phase of the SAP is where every hazard identified through the analysis and verification process is dispositioned against the final releasable design. The hazard items resolved and verified through design changes are statused as closed. All other hazard items are evaluated to ensure that they are acceptable prior to fleet release. The unresolved hazard items are then maintained for future design considerations.

2.1 SAFETY PROGRAM DEFINITION

Two primary items need to be defined within the safety program documentation to facilitate the SAP, organizational relationships and acceptable risk. These items are discussed below. For complete information on system safety program planning and the development of safety program planning documentation, refer to Task 102 of Reference 1.

2.1.1 Organization

In defining the safety program and associated responsibilities, an organizational outline is essential. The SAP relies heavily on information sharing and coordination throughout the system life-cycle. Without an understanding of how this gets accomplished organizationally, an integrated safety approach will fail to exist.

2.1.2 Definition of Acceptable Risk

In order to determine acceptable risk, risk must first be defined. Risk is defined as an expression of the possibility/impact of a mishap in terms of hazard severity and hazard probability (Reference 1). Figure 2 provides an example Risk Index Matrix used to define risk and acceptability. The definitions for categories and probabilities are defined in section 4.5 of Reference 1. The matrix with its associated acceptance criteria provides the groundwork for consistent safety evaluations within the weapon system. However, since equipment and

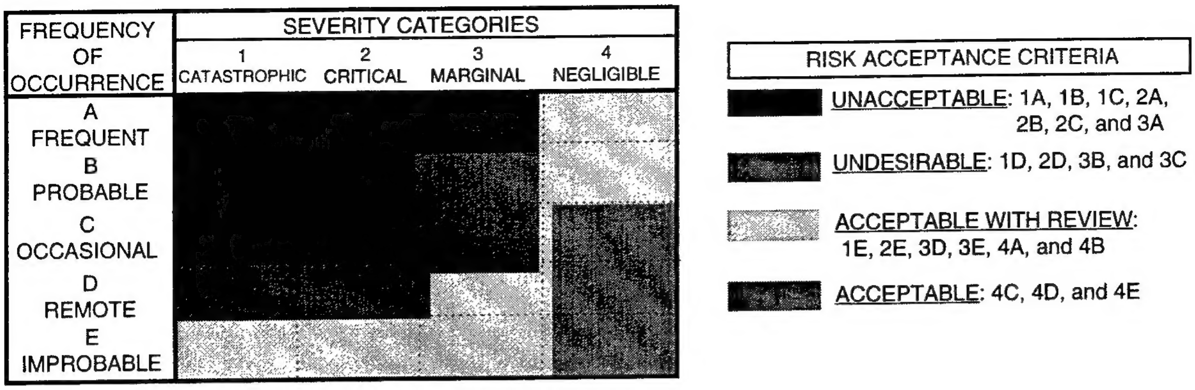

Figure 2. Risk Index Matrix / Risk Acceptance Criteria

environmental damage is often debatable in terms of severity, the matrix is effective only after the categories are clarified for the weapon system undergoing safety analysis. This clarification occurs during the preliminary hazard analysis, where specific weapon system hazards and mishaps are analyzed and associated severities documented.

2.2 IDENTIFICATION OF SAFETY CRITICAL ITEMS

The safety data items described in this section provide the necessary link between the real-life weapon system hazard and mishap considerations and the detailed analysis of a computer program. The information provides the intellect necessary to define safety critical events, safety critical processing, and safety critical data items within the computer programs. With these definitions, the CPSA methodology (defined later in this report) can then be utilized to verify the computer program design and implementation.

2.2.1 Derivation of the Event Criticality List

System level hazard analyses, as defined in this report, are analyses which identify hazardous states, assess component failures, assess failure modes, and identify and categorize risk, while assessing impacts to the environment, personnel, procedures, and equipment. The analyses often consider inherent hazards associated with explosives, radiation sources, pressure vessels, toxic materials, and high voltages during all modes of weapon system operation. They also consider the effects during all creditable environments (normal and abnormal) as well as the effects of human error, hardware failure, and combinations thereof. These system level hazard analysis efforts provide for the derivation of the ECL and ensure continuous validation of the ECL throughout the life of the weapon system.

Initial system level hazard analysis efforts generally include the development of a Preliminary Hazards List (PHL) and a Preliminary Hazard Analysis (PHA). The PHL is created during the weapon system concept phase as a mechanism to initiate the identification and tracking of hazards. The PHA expands on the PHL in identifying additional hazards and defining

specific hazard categories (i.e., severities). As a subset of the identified hazard items, an ECL should be developed. The ECL identifies specific weapon system operating modes, adverse safety events for those modes, and the associated severity. This list provides the mechanism for identifying and assessing weapon system safety considerations in the computer programs during detailed subsystem CPSA efforts. Since the ECL is developed to provide system safety related considerations for detailed CPSA, events and operating modes unrelated to computer programs should be omitted from the ECL (e.g., shipping, handling, disposal, etc.).

The ECL should focus on any adverse event which might occur during computer program execution, including events associated with weapon system installations, test events, operating modes, and training activities. Example items are shown in Table 1. Each item on the ECL should be categorized depending on the specifics of the weapon system and the operating mode for which the event occurs.

For example, a weapon system designed to withstand a restrained firing event might categorize the occurrence as a marginal event (minor equipment damage). However, a weapon system unable to withstand a restrained firing might categorize the occurrence as a critical or catastrophic event (major system damage or system loss respectively). In addition, operating modes need to be considered in categorizing the events. If the adverse event could reasonably result in fatalities during a training exercise, the event would be considered catastrophic. However, the same adverse event occurring in a tactical firing mode may not jeopardize the safety of personnel. In this case, the event would be assessed based on equipment and environmental damage, which would likely decrease the severity associated with that event.

2.2.2 Derivation of the Safety Critical Functions List

Safety Critical functions are identified during the PHA. These functions are normal events within the weapon system which are considered significant to safety, where significance is determined by the impact of improperly performing the function. The safety critical functions often relate to the release of energy, application of power, movement of mechanical devices, movement of physical objects, selection of ordnance, ordnance events, etc. In addition, functions such as the identification of ordnance, availability of ordnance, digital data loading, control of operating modes, operator actions, and training sequences can also be considered safety critical functions. Once identified, the safety critical functions are maintained as the CFL. An example CFL is provided as Table 2.

Within a weapon system, practically every function can be argued as safety critical. However, identifying every possible function as safety critical significantly reduces the effectiveness of the CPSA efforts. The goal in developing the CFL is to focus the detailed CPSA efforts, and allow concentration on safety critical processing areas and data items. If every function is considered safety critical, no focus is provided, and all processing is evaluated equally. This significantly increases the scope of the CPSA effort, and often decreases the effectively of the analysis. The end result is a degradation in the safety of the system due to lack of analysis concentration on safety critical areas.

Table 1. Example Event Criticality List

EVENT CRITICALITY LIST

MODE	EVENT	CATEGORY
All Modes	Inability to initiate fire protection	Catastrophic
	Fratricide	Catastrophic
	Operator confusion or lack of control : leads to catastrophic event	Catastrophic
	Operator confusion or lack of control : leads to critical event	Critical
	Inadvertent missile release (i.e., unre-strained missile)	Critical
	Operator confusion or lack of control: leads to marginal event	Marginal
	Inadvertent activation of fire protection	Marginal
	Inadvertent missile battery activation (i.e., Dud)	Marginal
Tactical Firing	Firing into no-fire zone	Catastrophic
	Restrained firing	Critical
	Inadvertent missile launch	Critical
	Inadvertent jettison	Marginal
	Inability to initiate safe sequencing	Marginal
	Exhaust gas intrusion into controlled area of ship	Marginal
	Premature missile arming	Negligible
Standby	Restrained firing	Catastrophic
	Inadvertent jettison	Catastrophic
	Inadvertent missile launch	Catastrophic
	Firing into no-fire zone	Catastrophic
	Inadvertent missile arming	Critical
Training	Restrained firing	Catastrophic
	Inadvertent jettison	Catastrophic
	Inadvertent missile launch	Catastrophic
	Firing into No-fire zone	Catastrophic
	Inadvertent missile arming	Catastrophic

Table 2. Example Critical Functions List

CRITICAL FUNCTIONS LIST	
CRITICAL FUNCTION	DESCRIPTION
Ordnance identification	The identification of ordnance through electrical interrogation after the ordnance is installed in the launching system.
Ordnance selection	The process of designating an ordnance item and establishing electrical connection.
Ordnance release	The initiation, transmission, and processing of electrical signal(s) that cause the ordnance to release from its restraint mechanism. Includes the monitoring functions associated with that process.
Booster/Rocket motor Arming	The initiation, transmission, and processing of electrical signal(s) that cause the booster/rocket motor to become armed. Includes the monitoring and safing functions associated with that process.
Booster/Rocket motor Ignition	The initiation, transmission, and processing that cause the booster/rocket motor to ignite.
Digital data download / transmission	The initiation, transmission, and processing of digital information which contributes to the activation of ordnance events or accomplishment of other critical functions.
Ordnance safing functions	The initiation, transmission, and processing of electrical signal(s) that cause the ordnance to return to a safe condition. Includes the monitoring functions associated with that process.
Launch/firing abort	The events and processing that restore ordnance to a safe condition following the decision to terminate a launch or firing event
System mode control	The events and processing that cause the weapon system to transition to a different operating mode and the proper use of electrical data items within that operating mode.
Response to hazard or mishap condition	The identification of hazardous conditions and the initiation, transmission, and processing of electrical signal(s) that mitigate or eliminate the hazard or mishap

2.3 DETAILED SAFETY ANALYSES

2.3.1 System Level Hazard Analyses

Several system level hazard analyses are performed throughout the life of the system. In performing the analyses and studying the analysis results, it is important to ensure that any discoveries which influence the ECL or CFL be documented. Any new information must then be factored into the CPSA effort for consideration of safety critical computer program processing. System level safety analyses which influence the ECL and CFL include, but are not limited to, Subsystem Hazard Analyses (SSHAs), Failure Modes and Hazardous Effects Analysis (FMHEAs), Operating and Support Hazard Analyses (O&SHAs), Fault Tree Analyses (FTAs), and Bent Pin Analyses. Basically, any analysis or study relating to the design or performance of the weapon system should be studied for ECL and CFL impacts.

2.3.2 Computer Program Safety Analysis

CPSA is performed to validate safety critical computer program processing. Figure 3 defines the methodology developed to perform this analysis. The non-shaded items in the figure represent those functions performed during the CPSA effort. The analysis approach consists primarily of requirements analysis, computer program design and code analysis, and safety testing. These processes are roughly sequential, with the results of requirements analysis providing much of the focus for design and code analysis efforts. Results and conclusions from requirements, design, and code analyses form the basis of the safety test effort. Consistent with system safety analyses, fault conditions, abnormal environments, abnormal responses, critical timing, and operator error are stressed when performing the analysis. As detailed analyses evolve, Safety Requirements (SRs) (as defined under CPSA Requirements Analysis) are continuously reviewed for their adequacy in ensuring weapon system safety, and updated as often as necessary.

During CPSA, all deficiencies discovered in the computer programs are recorded via Trouble Report. The Trouble Report documents the nature of the problem with the associated weapon system impacts. This report form is the vehicle utilized by the Configuration Management group to track and implement all outstanding issues against the weapon system computer programs. All groups or agencies, including those involved with the design, development, test, validation, safety, installation, and use of the weapon system document deficiencies and anomalies with this report form. If any of the submitted deficiencies represent a safety degradation, a detailed risk assessment (RA) is performed as a function of the CPSA effort. Each RA quantifies the risk associated with the specific deficiency, and provides detailed safety recommendations for mitigating the risk. These assessments are then used to justify and force safety related computer program design changes. This process is significant, since every recorded computer program deficiency or anomaly throughout the life of the weapon system is evaluated for safety impacts and associated risk. Details of performing computer program (RA) is discussed later in this section.

2.3.2.1 Requirements Analysis. There are two major objectives of the Computer Program Requirements Analysis. The first is to derive specific computer program SRs for the subsystem undergoing analysis. The second is to ensure that the specific computer program performance, design, and interface specifications provide for adequate safety given all operating modes and conditions.

The computer program SRs form the foundation for the entire CPSA effort. The SRs are developed by safety engineers to specify all performance related requirements within the subsystem necessary to ensure safety of the overall weapon system. These SRs are verified through analysis and test to ensure the safe operation and use of the computer programs for all environments and all operating modes. If the Computer Program design is found deficient such that a SR is violated, a computer program RA is generated and the design corrected to address the safety concern. The SRs are derived during requirements analysis and maintained throughout the CPSA period. This allows engineering data, analysis results, and test data to be evaluated against the existing SRs to continuously ensure adequate safety requirements exist to provide a safe computer program implementation.

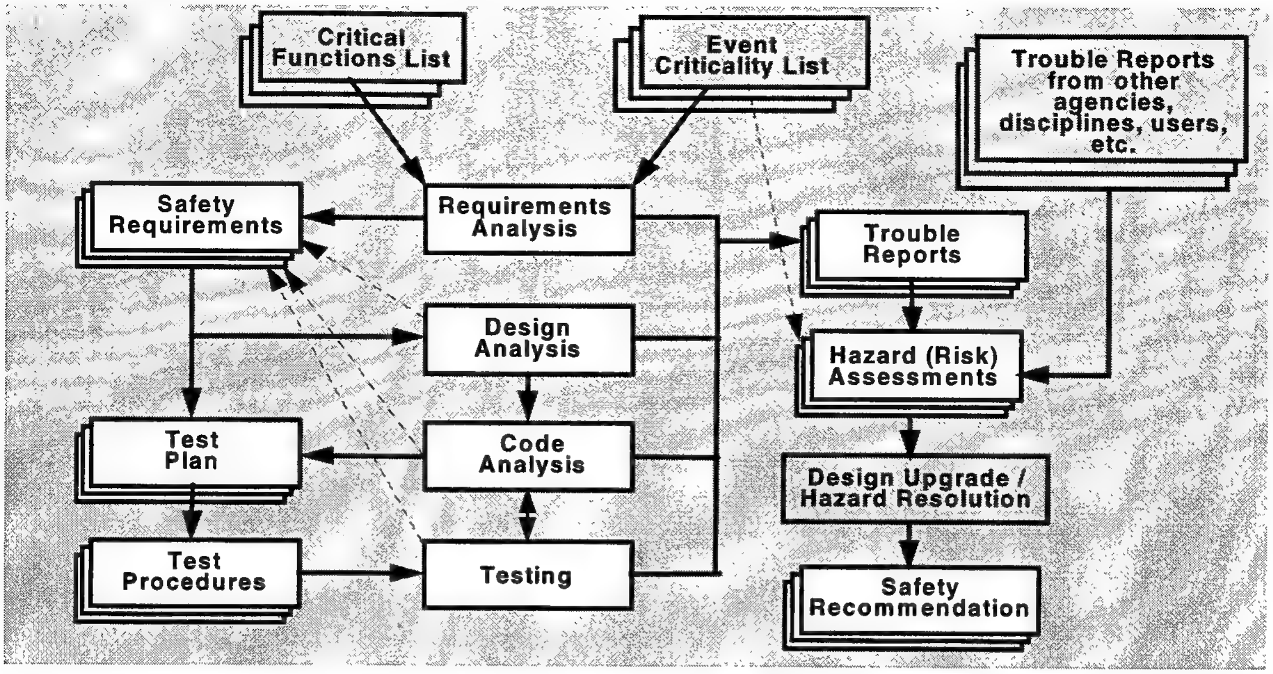

Figure 3. Computer Program Safety Analysis Methodology

SRs tend to focus on defining behavior that is critical to the safe operation of the system, hazardous to the personnel, or hazardous to the equipment or environment. Specifically, SRs for computer programs are derived to ensure:

(1) that the computer program performance does not cause the system to be placed in a hazardous state or create a hazardous condition,

(2) that if a hazardous state or condition is detected, the computer program responds to it and initiates action necessary to inform system operators of the condition and remove the system from the hazardous state or condition,

(3) that if operations are directly related to critical functions or the activation of energy or physical devices, the computer program allows the operations only when directed (if an external initiation is required) and only when the conditions for doing so are valid.

Detailed analysis of the design specifications (i.e., program performance specifications and interface design specifications) is conducted in parallel to the SR derivation process. This allows for the identification of safety related design specifications, and ensures those specifications are adequate to provide safe operation of the weapon system. This evaluation includes the identification of safety critical interface messages and safety critical data fields within those messages. If safety related deficiencies are identified for any of the design specifications, a change is initiated to address the safety concern. This approach provides for a complete definition of computer program safety design specifications before detailed design efforts and coding commence. In addition, when each individual safety related design specification, interface message, and data field is identified, future modifications or change proposals to the design specifications are easily assessed for safety applicability and impact.

Several items are necessary to adequately perform the requirements analysis. The top level system requirement document(s) (e.g., Prime Item Development Specification), program performance specification documents, and interface specifications must be utilized during the analysis. In addition, all safety specifications utilized in forming the safety program must be accessible. The ECL and CFL, as derived from the system level safety analyses, are also necessary for the requirements analysis effort. The importance of the ECL and CFL is significant. These lists provide the justification for defining specific SRs within the subsystem undergoing analysis, and provide for the identification of safety related design specifications. Without these safety data items, the CPSA effort will have limited or no focus on the safety critical processing within the weapon system.

2.3.2.2 Design and Code Analysis. Design and code analysis efforts make use of SRs, CFL, ECL, design specifications, schematics, and computer program source code drops for analysis purposes. The objective is to ensure detailed design and implementation of the weapon system specifications satisfy all SRs. In addition, this analysis ensures that the design and implementation of non-safety related functions do not interact with the performance of safety related functions or data items in ways that could degrade the overall safety of the weapon system. Tasks performed during design and code analysis include: Identification and evaluation of safety critical processing; identification and evaluation of safety critical data; verification of SRs; traceability analysis of design specification to source code; evaluation of critical timing; analysis of interrupts; and evaluation of the interface design.

During this analysis, specific design and implementation items are noted and considered for verification in detailed safety testing. These items relate to code segments which are difficult to verify through analysis, and therefore become candidates for the safety testing verification. Specific items include timing relationships, complex critical code segments, multi-tasking relationships, or unique computer program interactions. Since these design and implementation items are identified through analysis of the design and code, specific safety test scenarios can be developed to target the specific coding areas. In addition, each of the items identified are re-evaluated against the SRs to ensure the SRs provide adequate safety coverage despite the design complexity, timing relationships, interactions, or related concerns.

2.3.2.3 Testing. Computer program safety testing is the process of developing and executing test events while assessing weapon system performance. Testing scenarios often include no-go conditions, fault insertions, and hazard detection's, while operating under high levels of computer program load and stress. The tests provide a constant emphasis on safety and related functions while ensuring creditable conditions and scenarios. The intent is to elicit unsafe behavior under these conditions, and to stress complex and critical processing areas, force critically timed events, and exercise the critical aspects of multi-tasking implementations.

This testing approach is used to verify testable computer program SRs. Computer program predictability, in all operating modes and environments, is of the essence. This includes predictability in the computer programs response to external hazard conditions, weapon system faults, operator actions, and abnormal environments. The testing generally does not emphasize verification of performance requirements such as go-path sequences and go-path conditions.

However, go-path sequences and conditions do reflect safety critical processing, and therefore must be tested to ensure confidence in the safety critical functional areas.

2.3.2.4 Computer Program Risk Assessments. Each proposed enhancement or problem documented against the computer program, throughout the life of the weapon system, should be evaluated for safety related concerns. This includes documents submitted by internal or external groups, disciplines, agencies, or users. If the proposed enhancement or problem is determined to have a safety related concern, a computer program RA must be performed. Safety related concerns in the computer programs (herein referred to as deficiencies) can include code weaknesses, coding errors, unnecessary code, dead code, or problems incurred during test or use. The RA defines the details of the deficiency, all associated safety related impacts, the severity of these impacts, the probability of occurrence, and a detailed recommendation for resolving the deficiency. The assessment guidelines (i.e., severities, probabilities, and associated risk) are shown in Figure 2. The important aspect of performing a computer program RA is assessing the implementation within the weapon system and the risk introduced by inaccurate or incomplete computer program designs.

To properly perform the RA, system level safety analyses must be factored into the assessment. This is accomplished through the use of the ECL. The ECL provides insight on potential hazards and mishaps within the weapon system and provides the critical link between the system safety analysis conclusions and computer program assessments. This allows a focused assessment for the severity of the computer program hazard and its potential for creating a weapon system mishap.

The RA for each deficiency must address several items. Specifically, the RA should define the severity of the computer program hazard, probability that the hazard will occur, and its contribution to the probability of occurrence for an event on the ECL. This process essentially produces two separate risk indexes, one for the identified hazard and one for the ECL event, for use in prioritizing corrective action. This ensures both the computer program hazard and the weapon system safety impact are considered when determining the risk associated with the deficiency. The process for performing the RA is described below, followed by some example assessments.

Hazard Category: The hazard category is used to document the severity of the computer program hazard. The best approach in defining the hazard category associated the deficiency is to assess the hazard occurrence and the resulting equipment damage, environmental damage, or personnel injury. It is important to assess only the computer program hazard occurrence and the direct impact from that hazard at this time. The specific hazard occurrence and its influence on events documented in the ECL will be discussed as Event Severity later in this section. However, if the hazard occurrence directly causes an event documented on the ECL, the hazard category is equivalent to the category defined for that event on the ECL. For example: Assume an electrical ordnance identification check is incorporated in the system to ensure processing is performed on the intended ordnance item. If a deficiency exists such that the ordnance identification status goes unchecked during ordnance selection processing, but is checked and verified before the activation of irreversible ordnance functions, the hazard would be a category 4 hazard. The hazard is defined as failing to make a computer program safety interlock check, but

failure to make the check results in no specific damage or injury. Now, if the failure to properly identify the ordnance item allows processing to continue (i.e., an ordnance identification mismatch should have been detected and launch/firing terminated) such that electrical signals and commands are issued to an inappropriate ordnance item, the deficiency directly causes those signals to be inappropriately applied. The hazard severity in this case reflects the anticipated impact of inadvertent signal activation to the ordnance item. Likely, the severity will reflect events such as inadvertent battery activate, inadvertent launch, inadvertent release, or restrained firing. Finally, when assessing hazard severity, it is important to assess only additional damage or additional injury resulting from the deficiency if the weapon system is in a hazardous state or a mishap event has already occurred.

Hazard Probability: The hazard probability is used to document the probability that the hazard will occur. This evaluation must address the scenarios, external conditions, external influences, and any computer program limitations (e.g., processing speeds) to accurately define the probability for the hazard occurrence. For example, if a safety interlock ordnance identification check is erroneously omitted during normal processing, the probability of occurrence is frequent. However, if the check is omitted only after an external interface goes down within 500 milliseconds of two independent external events, the probability is reduced to a remote or improbable occurrence. Even though the computer program deficiency would occur each time (i.e., 100% of the time) these conditions exist, the true probability of that hazard occurring depends on the system level events.

Event Category: The Event Category documents the weapon system severity considerations for the identified hazard occurrence. The specific event and its severity are provided directly from the ECL. This evaluation is the process of determining which event on the ECL is most directly influenced by the computer program hazard occurrence. If the hazard occurrence can contribute to multiple events on the ECL, a determination should be made as to which is the most severe or most creditable. In determining credibility, the Event Probability (defined below) will have to be considered as well. As described in the Hazard Category discussion, it is acceptable to classify the event from the ECL as the same condition used in evaluating the hazard occurrence, when the hazard occurrence directly causes the event. For example, if the deficiency is that the computer program fails to command release of a missile after ignition, the hazard of failing to release directly causes a restrained firing event. In this case, the Event Category severity would be the same as the Hazard Category severity, a critical event per Table 2 for a restrained firing in firing mode.

Event Probability: The event probability is used to document the probability that an event from the ECL will occur. This evaluation addresses the influence of the hazard occurrence on the identified ECL event. The evaluation utilizes the hazard probability assessment and any remaining weapon system safety interlocks to assign an Event Probability. The safety interlocks considered can be functions of the computer program or designs external to the computer program. Safety interlocks are defined as any design or system components utilized to ensure safety of the system. This could be through physical isolation, positive checks, fail safe components, redundancy, sequence checks, integrity checks, etc. If no additional safety interlocks exist, the Event Probability is equivalent to the hazard probability since nothing additional in the design prohibits the hazard occurrence from causing the ECL event.

Upon completion of the defined evaluations, both the hazard risks and the event risks are compared against Table 2 for determination of acceptability within the weapon system. Those conditions producing the worst case risks provide the justifications which drive design changes for the identified computer program hazard. This risk evaluation process, which considers both hazard occurrence and ECL event, is derived from the Risk Assessment Procedure found in Ref 1. The Risk Assessment Procedure states that the evaluation shall be based upon the hazard probability, hazard severity, as well as risk impact, to establish the priority for corrective action and resolution of the identified hazard. Since risk impact refers to the assessment of mishaps, the ECL is used to factor in those considerations.

Example 1: For the ordnance identification deficiency described above, the status is not checked during nominal processing and failure to check does not result in any equipment damage, environmental damage, or personnel injury. Therefore, the hazard risk index associated with the deficiency is 4A per Table 2. The ECL event is evaluated based on an unintended ordnance item receiving specific signals and commands. Suppose the only other interlock prior to battery activate and missile release is for an operator to make a visual comparison prior to the next sequence command. However, multiple interlocks exist post missile release to identify the ordnance identification mismatch and prohibit rocket motor ignition and inadvertent launch of the ordnance item. Therefore the most creditable consideration is inadvertent missile release event, defined as a critical event per ECL (refer to Table 1). The probability for the event occurring factors in the remaining interlock of operator verification prior to battery activation and missile release. If an operator is prone to make an occasional error, the event risk index is 2C. Again, this assumes the hazard occurs every time, the only remaining system interlock is operator verification, and the operator makes errors occasionally. Therefore, per the Risk Assessment Procedure, the computer program hazard is considered unacceptable (2C) based on the risks associated with the ECL event of inadvertent missile release.

Example 2: Suppose a computer program deficiency exists where there is a remote possibility that an ordnance item is unnecessarily safed after its onboard batteries are activated. This creates a dud ordnance item within the weapon system. The deficiency creating this hazard occurrence actually causes equipment damage (i.e., expended batteries) and outgassing effects, which is considered marginal severity. The probability that the hazard will occur is based on the conditions which force the safing event, assessed as remote. Therefore the hazard risk index is 3D. The ECL event in this case is also inadvertent missile battery activate. Although battery activation was actually intended and the safing event was inadvertent, the resulting event is battery activation without launch. Since the ECL event is the same condition as the hazard occurrence, the Event Category is also marginal. In addition, the hazard occurrence directly causes the ECL event, so Event Probability equates to the Hazard Probability of remote. In this case, the hazard risk index and event risk index are the same (3D), so the computer program hazard is considered acceptable with review (3D) based on risks associated with the hazard of inadvertent safing after battery activate.

2.4 SAFETY DISPOSITION

The safety disposition is the composite safety assessment of all hazard items within the weapon system, including computer program deficiencies. Although every hazard item is considered, the assessment focuses on those hazard items assessed with a risk index of unacceptable, undesirable, or acceptable with review. Its likely that all unacceptable conditions are resolved at this point, since safety analyses directly influence the design throughout the design process to ensure these conditions are eliminated before release. Once the hazards items are reviewed, a recommendation concerning deployment can be made. To ease this process, it is recommended that accurate records for RAs and related design enhancements be maintained. This will facilitate an accurate safety disposition independent of the number of design changes, computer program builds, or deployed configurations throughout the life of the weapon system.

3.0 SUMMARY

The SAP, as defined in this report, provides a stable foundation for assessing computer programs and creates an integrated process for performing weapon system safety. The process facilitates evaluation consistency throughout the system life-cycle and supports a focused approach to CPSAs. In addition, the SAP provides a mechanism for accurately assessing the risk associated with computer program deficiencies. This is accomplished by enumerating both the computer program hazard occurrence and the resulting adverse safety event to accurately evaluate all safety considerations for the identified deficiency. With this integrated approach to system safety, fleet released computer programs are thoroughly evaluated to ensure a safe implementation into the weapon system. This provides the safest possible system to fleet personnel given all weapon system operating modes and environments.

4.0 REFERENCES

1. MIL-STD-882C, Military Standard, *System Safety Program Requirements*, Department of Defense, Washington, D.C.

DISTRIBUTION

	Copies
DOD ACTIVITIES (CONUS)	
ATTN CODE N713 (WRIGHT)	1
CODE N7135 (ANDREWS)	1
COMMANDER NAVAL ORDNANCE CENTER FARRAGUT HALL BLDG D323 INDIAN HEAD MD 20640-5100	
ATTN CODE 044D (HAMMER)	1
COMMANDER INDIAN HEAD DIVISION NAVAL SURFACE WARFARE CENTER 101 STRAUSS AVENUE BLDG 482 INDIAN HEAD MD 20640-5000	
ATTN SPAWAR 20-22 (ANDERSON)	1
COMMANDER SPACE AND NAVAL WARFARE SYSTEMS COMMAND 2451 CRYSTAL DRIVE CRYSTAL PARK 5 ARLINGTON VA 22245-5200	
ATTN PMS422-311 (LISZNIANSKY)	1
PROGRAM EXECUTIVE OFFICE THEATER AIR DEFENSE 2531 JEFFERSON DAVIS HWY ARLINGTON VA 22242-5170	
ATTN CODE C2622 (CHIRKIS)	1
CODE 41J000D (BANISTER)	1
COMMANDER NAVAL AIR WARFARE CENTER WEAPONS DIVISION BLDG 1 ADMINISTRATION CIRCLE CHINA LAKE CA 93555	
ATTN CODE N535 (IANSON)	1
CODE DN211 (ROSTOSKY)	1
NATO SEASPARROW PROGRAM OFFICE 2531 JEFFERSON DAVIS HIGHWAY ARLINGTON VA 22242-5170	
ATTN CODE 4D20 (MARCOUX)	1
CODE 4D23 (SCHULTZEL)	1
COMMANDER NAVAL SURFACE WARFARE CENTER PORT HUENEME DIVISION PORT HUENEME CA 93043-5007	
ATTN CODE A76 (TECH LIBRARY)	1
CODE 20	1
CODE 30	1
COMMANDING OFFICER CSSDD NSWC 6703 W HIGHWAY 98 PANAMA CITY FL 32407-7001	
DEFENSE TECH INFORMATION CTR 8725 JOHN J KINGMAN RD SUITE 0944 FORT BELVOIR VA 22060-6218	2
NON-DOD ACTIVITIES (CONUS)	
ATTN J BOZARTH	1
EG&G WASC INC 16156 DAHLGREN ROAD PO BOX 552 DAHLGREN VA 22448	
ATTN J DAWSON	1
VITRO CORPORATION CRYSTAL PARK 3 2231 CRYSTAL DRIVE SUITE 600 ARLINGTON VA 22202	

DISTRIBUTION (CONTINUED)

	Copies
ATTN HOWARD CARSTENS UNITED DEFENSE LP ARMAMENT SYSTEMS DIVISION 4800 EAST RIVER ROAD MINNEAPOLIS MN 55459-0043	1
ATTN STEVENS PAYNE COMPUTER SCIENCES CORPORATION 601 CAROLINE STREET SUITE 700 FREDERICKSBURG VA 22401	1
ATTN JANET GILL 21 ALLSTON LANE HOLLYWOOD MD 20636	1
ATTN MS HYLAND 23343 WILDEWOOD BLVD CALIFORNIA MD 20619	1
ATTN DOUG WIETZKE VITRO CORPORATION 45 WEST GUDE DRIVE ROCKVILLE MD 20850-1160	1
ATTN JIM TURNER HUGHES MISSILE COMPANY PO BOX 11337 TUCSON AZ 85734-1337	1
ATTN GENE DESANTIS LOCKHEED MARTIN 103 CHESAPEAKE PARK PLAZA BALTIMORE MD 21220	1
ATTN SEMI (HOLBROOK) HUGHES MISSILE COMPANY PO BOX 11337 TUCSON AZ 85734-1337	1
ATTN MIKE CLAYPOOL MCDONNELL DOUGLAS P O BOX 516 ST LOUIS MO 63116-0516	1
THE CNA CORPORATION P O BOX 16268 ALEXANDRIA VA 22302-0268	1

	Copies
ATTN GIFT AND EXCHANGE DIVISION LIBRARY OF CONGRESS WASHINGTON DC 20540	4
ATTN MS M E CARO APPLIED ORDNANCE TECHNOLOGY 1735 JEFFERSON DAVIS HIGHWAY SUITE 1000 CRYSTAL SQUARE #3 ARLINGTON VA 22202-3401	1

INTERNAL

B		1
B60	(LIBRARY)	1
D		1
G		1
G21	(DINEEN)	1
G70		1
G71		35
G71	(ZEMORE)	1
G72		1
J		1
K		1
N		1
N93	(HORNER)	1
T		1